

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

2
3
4

6
7
8
9
10
11
12
13
14

16
1718
19

20
21
22
23
24
25

26
27

1 5. The method of claim 4 wherein at least some of the
2 statistical information is contained in a state table.

3 6. The method of claim 4 wherein a plurality of retrieval
4 commands are issued, and the statistical information comprises at
5 least one of the following:

6 rate of retrieving rows from the computer code;

7 rate of retrieving columns from the computer code;

8 rate of retrieving tables from the computer code;

9 average number of rows retrieved per retrieval command

10 for a given input vector, where an input vector

11 contains parameterized information characteristic of

12 the retrieval command;

13 average number of columns retrieved per retrieval

14 command for a given input vector;

15 average number of tables retrieved per retrieval

16 command for a given input vector;

17 percentage of retrieval commands for which a given

18 column is accessed;

19 percentage of retrieval commands for which a given

20 table is accessed;

21 percentage of retrieval commands for which a given

22 combination of columns is accessed;

23 percentage of retrieval commands for which a given

24 combination of tables is accessed.

1 7. The method of claim 1 wherein said at least one rule is
2 also accessed by an input vector containing parameterized
3 information characteristic of the retrieval command.

4 8. The method of claim 7 wherein the input vector is
5 extracted from a retrieval command by at least one technique from
6 the group of techniques comprising real-time auditing and in-line
7 interception.
8

9 9. The method of claim 7 wherein said at least one rule is
10 accessed by at least two input vectors, each input vector being
11 associated with the same retrieval command.

12 10. The method of claim 7 wherein the input vector comprises
13 at least one parameter from the group of parameters comprising:

14 canonicalized commands;

15 dates and times at which commands access the computer
16

17 code;

18 logins of users that issue commands;

19 identities of users that issue commands;

20 departments of users that issue commands;

21 applications that issue commands;

22 IP addresses of issuing users;

23 identities of users accessing a given field within the
24

25 computer code;

26 times of day that a given user accesses a given field
27

27 within the computer code;

28

1 fields accessed by commands;
2 combinations of fields accessed by commands;
3 tables within the computer code accessed by commands;
4 combinations of tables within the computer code
5 accessed by commands.

6 11. The method of claim 10 wherein a canonicalized command
7 is a retrieval command stripped of literal field data.
8

9 12. The method of claim 1 wherein, when a retrieval command
10 is flagged as suspicious, at least one of the following is
11 performed:

12 an alert is sent to a system administrator;
13 an audit log is updated;
14 the command is not allowed to access the computer code;
15 the command is allowed to access the computer code, but
16 the access is limited;
17 the command is augmented;
18 a sender of the command is investigated.

19 13. The method of claim 1 wherein the computer code is a
20 database.
21

22 14. The method of claim 13 wherein the retrieval command is
23 a SQL command.
24

25 15. The method of claim 1 wherein said at least one rule
26 contains content developed during a training phase.
27

1 16. The method of claim 15 wherein said at least one rule
2 comprises at least one rule derived from statistical information
3 accumulated during the training phase.

4 17. The method of claim 15 wherein the training phase is
5 performed in real time.

6 18. The method of claim 15 wherein the training phase
7 comprises the steps of:
8

9 observing retrieval commands that access the computer
10 code;

11 observing responses to the retrieval commands generated
12 by the computer code; and

13 deriving from said responses a set of retrieval
14 information.

15 19. The method of claim 18 wherein the step of observing
16 retrieval commands comprises at least one of:
17

18 real-time auditing; and

19 in-line interception.

20 20. The method of claim 19 wherein the step of observing
21 retrieval commands comprises real-time auditing; and at least one
22 of the following is used to extract the commands for observation:

23 an API that accesses the computer code;

24 code injection;

25 patching;

26 direct database integration;
27
28

1 log file examination.

2 21. The method of claim 19 wherein the step of observing
3 retrieval commands comprises in-line interception; and at least
4 one of the following is interposed between senders of the
5 commands and the computer code:

6 a proxy;
7 a firewall;
8 a sniffer.

10 22. The method of claim 18 wherein the step of observing
11 responses to the retrieval commands comprises at least one of:

12 real-time auditing; and
13 in-line interception.

14 23. The method of claim 22 wherein the step of observing
15 responses to the retrieval commands comprises real-time auditing;
16 and at least one of the following is used to extract the commands
17 for observation:

18 an API that accesses the computer code;
19 code injection;
20 patching;
21 direct database integration;
22 log file examination.

24 24. The method of claim 22 wherein the step of observing
25 responses to the retrieval commands comprises in-line
26

1 interception; and at least one of the following is interposed
2 between senders of the commands and the computer code:

3 a proxy;
4 a firewall;
5 a sniffer.
6

7 25. The method of claim 15 wherein a duration of performing
8 the training phase is determined by statistical means.

9 26. The method of claim 15 wherein:

10 during the training phase, suspicious activity is
11 tracked; and

12 the suspicious activity is subsequently reported to a
13 system administrator.
14

15 27. The method of claim 1 wherein the generating step
16 comprises at least one of:

17 real-time auditing; and
18 in-line interception.

19 28. The method of claim 1 wherein said at least one rule
20 comprises at least one rule provided by a system administrator.

21 29. The method of claim 1 wherein said at least one rule
22 comprises at least one rule provided by a vendor.
23

24 30. The method of claim 1 wherein said at least one rule
25 comprises a pre-established rule table pertaining to retrievals.

26 31. A computer-readable medium containing computer program
27 instructions for protecting computer code from malicious
28

1 retrievers, said computer program instructions performing the
2 steps of:

3 generating retrieval information characteristic of data
4 sent to a retriever by the computer code in response
5 to a retrieval command issued by the retriever;
6 accessing at least one rule using at least some of said
7 retrieval information as an input to said at least
8 one rule; and
9 when said at least one rule informs that the retrieval
10 is not acceptable, flagging the retrieval command as
11 suspicious.
12

13 32. Apparatus for protecting computer code from malicious
14 retrievers, said apparatus comprising:

15 means for generating retrieval information
16 characteristic of data sent to a retriever by the
17 computer code in response to a retrieval command
18 issued by the retriever;
19 coupled to the generating means, at least one rule
20 pertaining to retrievals; and
21 means for accessing said at least one rule using
22 retrieval information as an input to said at least
23 one rule.
24
25
26
27
28